

© 2006 The Authors

**DEFENDANT GOOGLE LLC’S MOTION FOR SUMMARY JUDGMENT
OF NON-INFRINGEMENT**



TABLE OF CONTENTS

	Page
INTRODUCTION AND SUMMARY OF ARGUMENT	1
ARGUMENT	1
I. THE PLAIN AND ORDINARY MEANING OF “DEEP PACKET INSPECTION” REQUIRES MONITORING BOTH THE HEADER AND PAYLOAD OF A PACKET	1
II. THERE IS NO EVIDENCE TO SHOW THAT THE ACCUSED PRODUCTS MONITOR THE HEADER AND PAYLOAD OF PACKETS SENT BY SUBSCRIBERS	3
CONCLUSION	4



TABLE OF AUTHORITIES

Page

CASES

Oscar Renda Contracting, Inc. v. City of Lubbock,
2008 WL 11429735 (N.D. Tex. 2008)..... 3

** Emphasis added throughout unless indicated otherwise.*

*** Deposition objections removed unless indicated otherwise.*

**TABLE OF EXHIBITS**

Exhibit No.	Description
1	U.S. Patent 8,041,806
2	2023-06-08 Deposition of W. Mangione Smith
3	H. Hough Rebuttal Non-Infringement Report
4	2023-02-22 Deposition of A. Kushnir
5	Deposition Ex. DX005 to W. Mangione Smith Deposition
6	Deposition Ex. DX006 to W. Mangione Smith Deposition
7	Deposition Ex. DX007 to W. Mangione Smith Deposition
8	Deposition Ex. DX008 to W. Mangione Smith Deposition

INTRODUCTION AND SUMMARY OF ARGUMENT

Dependent claim 3 is the only remaining claim in this case. It recites “*a Deep Packet Inspection (DPI)* module ... operable to monitor the access communication traffic.” (Ex. 1, 16:50-52). Deep packet inspection was a well-known term before the filing date of asserted U.S. Patent No. 8,041,806 (“the ’806 patent”). (Ex. 2 at 26:25–27:14). The testimony of plaintiff’s expert (Dr. Mangione-Smith) and his own prior-art publications establish that the ordinary meaning of the term “deep packet inspection” requires monitoring *both* the header and payload portions of a packet. *See* Section I. The header typically includes the source and destination addresses of the packet and the payload includes the data. (Ex. 2 at 14:17-15:8; Ex. 3 at ¶ 128).

The parties have completed fact and expert discovery, and plaintiff still cannot identify any evidence that the accused YouTube TV and Google TV products monitor both the header and payload portions of the actual packets sent by a subscriber. Indeed, plaintiff’s expert concedes that “header” and “payload” do not appear in his report’s analysis. Plaintiff’s expert also admits that he has not seen the terms “deep packet inspection” or “DPI” [REDACTED]. This is not surprising because Google’s corporate representative made clear that neither accused product uses DPI. (Ex. 4 at 117:15-23). On this record, no genuine dispute exists that the accused products do not implement “deep packet inspection” and thus cannot infringe. *See* Section II.

ARGUMENT

I. THE PLAIN AND ORDINARY MEANING OF “DEEP PACKET INSPECTION” REQUIRES MONITORING BOTH THE HEADER AND PAYLOAD OF A PACKET

Claim 3 recites “a Deep Packet Inspection (DPI) module operatively coupled to the behavioral information collector and operable to monitor the access communication traffic.” (Ex. 1, 16:50-52). The term “deep packet inspection” is a term of art that existed before the priority date (September 2006) of the ’806 patent, and it had an established ordinary meaning. (Ex. 2 at 22:5-14, 26:25–27:14). As



multiple publications from plaintiff's own expert uniformly demonstrate, "deep packet inspection" requires examining both the header and the payload of the packet. In a 2005 publication, plaintiff's expert (Dr. Mangione-Smith) wrote that application-level network attacks "can be more accurately detected *by a technique termed* Deep Packet Inspection." (Ex. 5 at 1). Plaintiff's expert then explained: "Deep packet inspection *not only* examines headers *but also* the payloads of packets." (*Id.*) In the same article, plaintiff's expert stated that "[d]eep packet inspection *not only* examines the packet header, *but also* looks through the entire payload searching for all the user specified patterns." (*Id.*) Likewise, in a 2004 publication, plaintiff's expert explained: "Deep packet filters are designed to *not only* examine headers *but also* the payloads of the packets." (Ex. 6 at 1). In another 2005 publication, plaintiff's expert again explained:

An effective security measure for such attack is deep packet inspection. Deep packet inspection *not only* examines the packet headers *but also* the payload data.

(Ex. 7 at 1). Other prior art further confirms that "deep packet inspection" requires examining both the header and payload in the packets sent by a subscriber. (Ex. 8, 3:33-38 (describing use of "*common* inspection technology such as *deep packet inspection (DPI) which can analyze packet traffic ...* such as packet *headers and payloads* to assess the behavior of a target end user"))).

During his deposition, plaintiff's expert confirmed that "deep packet inspect" involves monitoring both the header and payload in a packet. Testifying about his publication from 2005, plaintiff's expert explained:

Q. And in the next sentence you wrote that: "Deep packet inspection not only examines the packet headers but also the payload data"; correct?

A. Yes. I see that, and *that is my understanding still.*

(Ex. 2 at 50:24-51:3) (testifying about Ex. 6). Plaintiff's expert further explained:

Q. And in the second sentence under the section titled "Introduction," you wrote that: "Deep packet inspection not only examines headers but also the payloads of the

[REDACTED]

packets”; correct?

A. Yes ... I think that’s probably a better comment *on what DPI is*.

(*Id.* at 41:22-42:2 (testifying about Ex. 5)). And plaintiff’s expert confirmed that “deep packet inspection” monitors the *actual* packets sent, including the header and payload:

Q. Would deep packet inspection monitor the actual packets that were sent on the internet?

A. *Yes. That was the intention.* Although simply monitoring the packets sent on the internet was an older technology as well that was done without the need for DPI.

Q. Would deep packet inspection monitor the actual header and actual payload of the packets that were sent on the internet?

A. *Yes, that was—that’s the intention.*

(*Id.* at 49:16-25). Similarly, Google’s expert Dr. Houh also explained that “deep packet inspection” requires monitoring both the header and payload of the packets sent on a network. (Ex. 3 at ¶¶ 131-40).

In sum, the plain and ordinary meaning of “deep packet inspection” requires monitoring both the header and payload of a packet.

II. THERE IS NO EVIDENCE TO SHOW THAT THE ACCUSED PRODUCTS MONITOR THE HEADER AND PAYLOAD OF PACKETS SENT BY SUBSCRIBERS

“[S]ummary judgment is essentially ‘put up or shut up’ time for the non-moving party.” *Oscar Renda Contracting, Inc. v. City of Lubbock*, 2008 WL 11429735, at *15 (N.D. Tex. 2008). With fact and expert discovery closed, plaintiff has a complete failure of proof to show that the accused YouTube TV and Google TV products perform deep packet inspection.

Plaintiff’s expert admits that he did not identify any Google document or any source code that [REDACTED] (Ex. 2 at 159:4-160:24). And despite confirming his understanding that “deep packet inspection” requires monitoring both the header and payload of the packets sent by a subscriber, plaintiff’s expert concedes that the analysis in his report never mentions a

[REDACTED]

“header” or “payload.” (*Id.* at 244:16-245:12). Similarly, Google’s expert explained that “Google’s

[REDACTED]” “packet

headers [REDACTED]

[REDACTED]” and plaintiff’s expert “presented no opinion or evidence that the accused

products [REDACTED].” (Ex. 3 ¶¶ 155-56).

The reason for the absence of any evidence regarding “deep packet inspection” is straightforward: The accused YouTube TV and Google TV products simply *do not do it*. As Google’s corporate representative made clear:

Q. Is the information that Anima provides to YouTube TV and Google TV obtained

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

(Ex. 4 at 117:15-23).

CONCLUSION

For the reasons above, Google respectfully asks this Court to grant summary judgment of non-infringement as to asserted claim 3 of the ’806 patent.

Date: June 28, 2023

Respectfully submitted,

*/s/ T. Gregory Lanier, with permission by
Shaun W. Hassett*

T. Gregory Lanier (*pro hac vice*)
Jones Day
1755 Embarcadero Road
Palo Alto, California, 94303
+1 (650) 739-3939
+1 (650) 739-3900 facsimile
tglanier@jonesday.com

Michael E. Jones (Texas Bar No. 10929400)
Shaun W. Hassett (Texas Bar No. 24074372)
Potter Minton, P.C.
102 North College, Suite 900
Tyler, Texas, 75702
+1 (903) 597-8311
+1 (903) 593-0846 facsimile
mikejones@potterminton.com
shaunhassett@potterminton.com

Sasha Mayergoyz
Jones Day
77 W. Wacker Drive
Chicago, IL 60601
+1 (312) 782-3939
smayergoyz@jonesday.com

Tracy A. Stitt
Edwin O. Garcia
Jones Day
51 Louisiana Avenue NW
Washington, DC 20001
+1 (202) 879-3641
tastitt@jonesday.com
edwingarcia@jonesday.com

Michael A. Lavine
Jones Day
555 California Street, 26th Floor
San Francisco, California 94104
+1 (415) 626-3939
mlavine@jonesday.com

Attorneys for Defendant Google LLC

CERTIFICATE OF SERVICE

I hereby certify that all counsel of record who have consented to electronic service are being served with a copy of this document via electronic mail on June 28, 2023.

I also hereby certify that all counsel of record who have consented to electronic service are being served with a notice of filing of this document, under seal, pursuant to L.R. CV-5(a)(7) on June 28, 2023.

/s/ Shaun W. Hassett